INTERNAL REVENUE SERVICE
IRS Fact Sheet

- Media Relations Office Washington, D.C. Media Contact: 202.622.4000

www.IRS.gov/newsroom Public Contact: 800.829.1040

Online Scams that Impersonate the IRS

Video: Phishing-Malware: English

FS-2010-9, January 2010

WASHINGTON — Consumers should protect themselves against online identity theft and other scams that increase during and linger after the filing season. Such scams may appropriate the name, logo or other appurtenances of the IRS or U.S. Department of the Treasury to mislead taxpayers into believing that the scam is legitimate.

Scams involving the impersonation of the IRS usually take the form of e-mails, tweets or other online messages to consumers. Scammers may also use phones and faxes to reach intended victims. Some scammers set up phony Web sites.

The IRS and E-mail

Generally, the IRS does not send unsolicited e-mails to taxpayers. Further, the IRS does not discuss tax account information with taxpayers via e-mail or use e-mail to solicit sensitive financial and personal information from taxpayers. The IRS does not request financial account security information, such as PIN numbers, from taxpayers.

Object of Scams

Most scams impersonating the IRS are identity theft schemes. In this type of scam, the scammer poses as a legitimate institution to trick consumers into revealing personal and financial information — such as passwords and Social Security, PIN, bank account and credit card numbers — that can be used to gain access to and steal their bank, credit card or other financial accounts. Attempted identity theft scams that take place via e-mail are known as phishing. Other scams may try to persuade a victim to advance sums of money in the hope of realizing a larger gain. These are known as advance fee scams.

Who Is Targeted

Anyone with a computer, phone or fax machine could receive a scam message or unknowingly visit a phony or misleading Web site. Individuals, businesses, educators, charities and others have been targeted by e-mails that claim to come from the IRS or Treasury Department. Scam e-mails are generally sent out in bulk, based on e-mail addresses (urls), similar to spam.

How an Identity Theft Scam Works

Most of the scams that impersonate the IRS are identity theft scams. Typically, a consumer will receive an e-mail that claims to come from the IRS or Treasury Department. The message will

contain an enticing or intimidating subject line, such as tax refund, inherited funds or IRS notice. Usually, the message will state that the recipient needs to provide the IRS with information to obtain the refund or avoid some penalty. The message will instruct the consumer to open an attachment or click on a link in the e-mail. This may lead to an official-looking form to be filled out online or send the taxpayer to a seemingly genuine but bogus IRS Web site. The look-alike site will then contain a phony but genuine-looking online form or interactive application that requires the personal and financial information the scammer can use to commit identity theft.

Alternatively, the clicked link may secretly download malware to the consumer's computer. Malware is malicious code that can take over the computer's hard drive, giving the scammer remote access to the computer, or it could look for passwords and other information and send them to the scammer.

Phony Web or Commercial Sites

In many IRS-impersonation scams, the scammer sends the consumer to a phony Web site that mimics the appearance of the genuine IRS Web site, IRS.gov. This allows the scammer to steer victims to phony interactive forms or applications that appear genuine but require the targeted victim to enter personal and financial information that will be used to commit identity theft.

The official Web site for the Internal Revenue Service is IRS.gov, and all IRS.gov Web page addresses begin with http://www.irs.gov/.

In addition to Web sites established by scammers, there are commercial Internet sites that often resemble the authentic IRS site or contain some form of the IRS name in the address but end with a .com, .net, .org or other designation instead of .gov. These sites have no connection to the IRS. Consumers may unknowingly visit these sites when searching the Internet to retrieve tax forms, publications and other information from the IRS.

Frequent or Recent Scams

There are a number of scams that impersonate the IRS. Some of them appear with great frequency, particularly during and right after filing season, and recur annually. Others are new.

- **Refund Scam** — This is the most frequent IRS-impersonation scam seen by the IRS. In this phishing scam, a bogus e-mail claiming to come from the IRS tells the consumer that he or she is eligible to receive a tax refund for a specified amount. It may use the phrase "last annual calculations of your fiscal activity." To claim the tax refund, the consumer must open an attachment or click on a link contained in the e-mail to access and complete a claim form. The form requires the entry of personal and financial information. Several variations on the refund scam have claimed to come from the Exempt Organizations area of the IRS or the name and signature of a genuine or made-up IRS executive. In reality, taxpayers do not complete a special form to obtain their federal tax refund — refunds are triggered by the tax return they submitted to the IRS.

- **Lottery winnings or cash consignment** — These advance fee scam e-mails claim to come from the Treasury Department to notify recipients that they'll receive millions of dollars in recovered funds or lottery winnings or cash consignment if they provide certain personal information, including phone numbers, via return e-mail. The e-mail may be just the first step in a multi-step scheme, in which the victim is later contacted by telephone or

further e-mail and instructed to deposit taxes on the funds or winnings before they can receive any of it. Alternatively, they may be sent a phony check of the funds or winnings and told to deposit it but pay 10 percent in taxes or fees. Thinking that the check must have cleared the bank and is genuine, some people comply. However, the scammers, not the Treasury Department, will get the taxes or fees. In reality, the Treasury Department does not become involved in notification of inheritances or lottery or other winnings.

- **Beneficial Owner Form** — This fax-based phishing scam, which generally targets foreign nationals, recurs periodically. It's based on a genuine IRS form, the W-8BEN, Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding. The scammer, though, invents his or her own number and name for the form. The scammer modifies the form to request passport numbers, information that is often used for account security purposes (such as mother's maiden name) and similar detailed personal and financial information, and states that the recipient may have to pay additional tax if he or she fails to immediately fax back the completed form. In reality, the real W-8BEN is completed by banks, not individuals.

Other Known Scams

The contents of other IRS-impersonation scams vary but may claim that the recipient will be paid for participating in an online survey or is under investigation or audit. Some scam e-mails have referenced Recovery-related tax provisions, such as Making Work Pay, or solicited for charitable donations to victims of natural disasters. Taxpayers should beware of an e-mail scam that references underreported income and the recipient's "tax statement," since clicking on a link or opening an attachment is known to download malware onto the recipient's computer.

How to Spot a Scam

Many e-mail scams are fairly sophisticated and hard to detect. However, there are signs to watch for, such as an e-mail that:

- Requests detailed or an unusual amount of personal and/or financial information, such as name, SSN, bank or credit card account numbers or security-related information, such as mother's maiden name, either in the e-mail itself or on another site to which a link in the e-mail sends the recipient.

- Dangles bait to get the recipient to respond to the e-mail, such as mentioning a tax refund or offering to pay the recipient to participate in an IRS survey.

- Threatens a consequence for not responding to the e-mail, such as additional taxes or blocking access to the recipient's funds.

- Gets the Internal Revenue Service or other federal agency names wrong.

- Uses incorrect grammar or odd phrasing (many of the e-mail scams originate overseas and are written by non-native English speakers).

- Uses a really long address in any link contained in the e-mail message or one that does not start with the actual IRS Web site address (http://www.irs.gov). The actual link's

address, or url, is revealed by moving the mouse over the link included in the text of the e-mail.

What to Do

Taxpayers who receive a suspicious e-mail claiming to come from the IRS should take the following steps:

- Avoid opening any attachments to the e-mail, in case they contain malicious code that will infect your computer.

- Avoid clicking on any links, for the same reason. Alternatively, the links may connect to a phony IRS Web site that appears authentic and then prompts for personal identifiers, bank or credit card account numbers or PINs.

- Visit the IRS Web site, www.irs.gov, to use the "Where's My Refund?" interactive tool to determine if they are really getting a refund, rather than responding to the e-mail message.

- Forward the suspicious e-mail or url address to the IRS mailbox phishing@irs.gov, then delete the e-mail from their inbox.

Consumers who believe they are or may be victims of identity theft or other scams may visit the U.S. Federal Trade Commission's Web site for identity theft, www.OnGuardOnline.gov, for guidance in what to do. The IRS is one of the sponsors of this site.

More information on IRS-impersonation scams, identity theft and suspicious e-mail is available on IRS.gov.